

日本の「AI事業者ガイドライン（第1.2版）」：実務対応の最前線

第1.2版の核心：定義の拡張とリスクの再定義

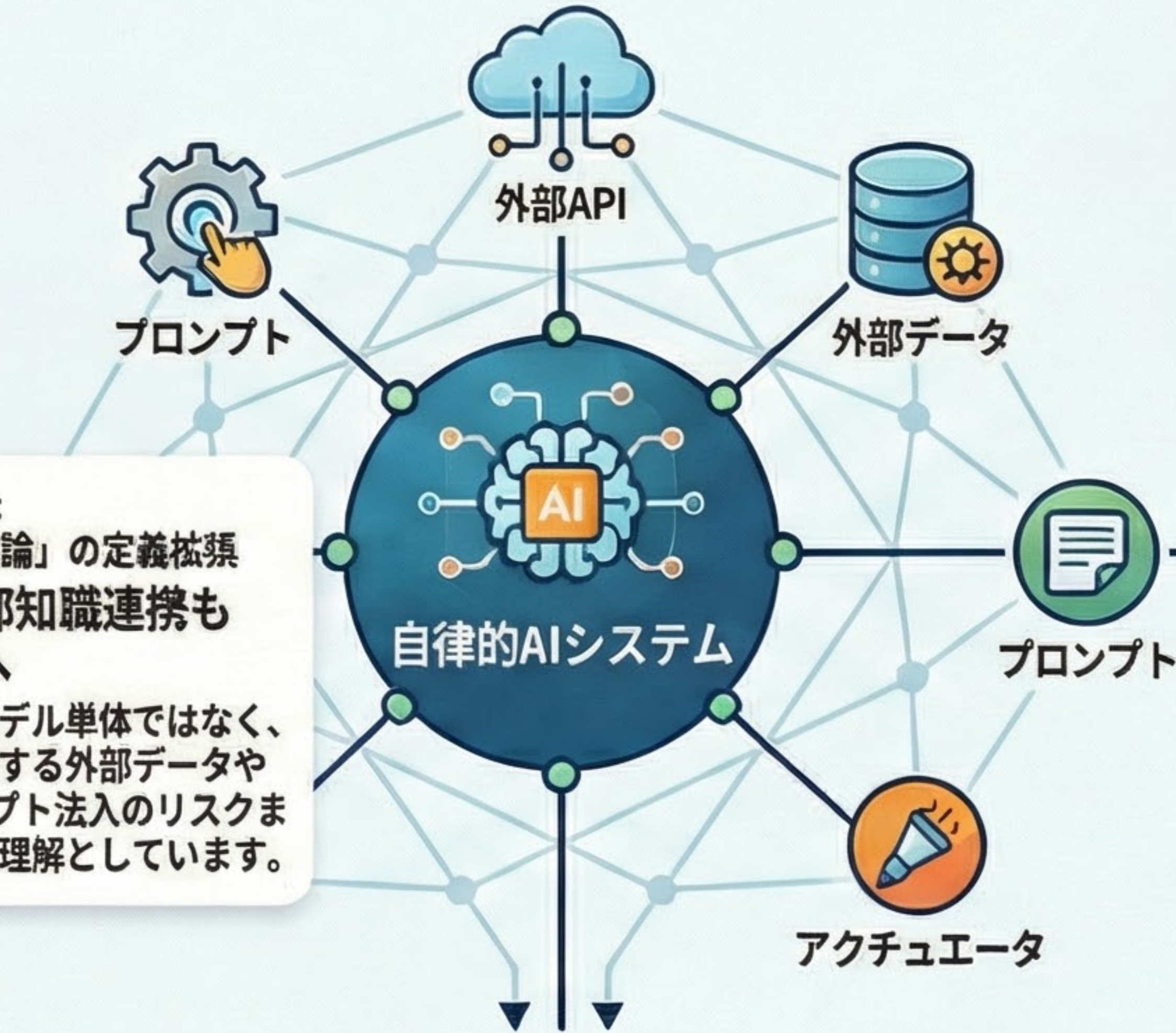


DEFINITION: AIエージェント
自律的に行動するAIシステム
 特定の目標達成のために環境を感知し、自律的に権限を行登する（自欺特法、迷金等）システムを定義し、責任分配の明確化を求めています。



DEFINITION: フィジカルAI
物理世界に直接作用するAI
 アクチュエータを介して現実世界に働きかけるAIを揺し、サイバー空間だけでなく人身・説覧への危害防止を最優先事項としています。

KEY_FINDING:
 「学習」「推論」の定義拡張
RAGや外部知識連携も管理対象へ
 リスク度をモデル単体ではなく、推諫的に参照する外部データやAPI、プロンプト法入のリスクまで含めて共通理解としています。



業界別：対応コストと追加負担の目安



STATISTIC: 製造業（ロボット・検査）
追加負担：約130万～820万円
 安全性権掲や停止基準の實定のため、年間3～12人月の追加工数が想定されます。

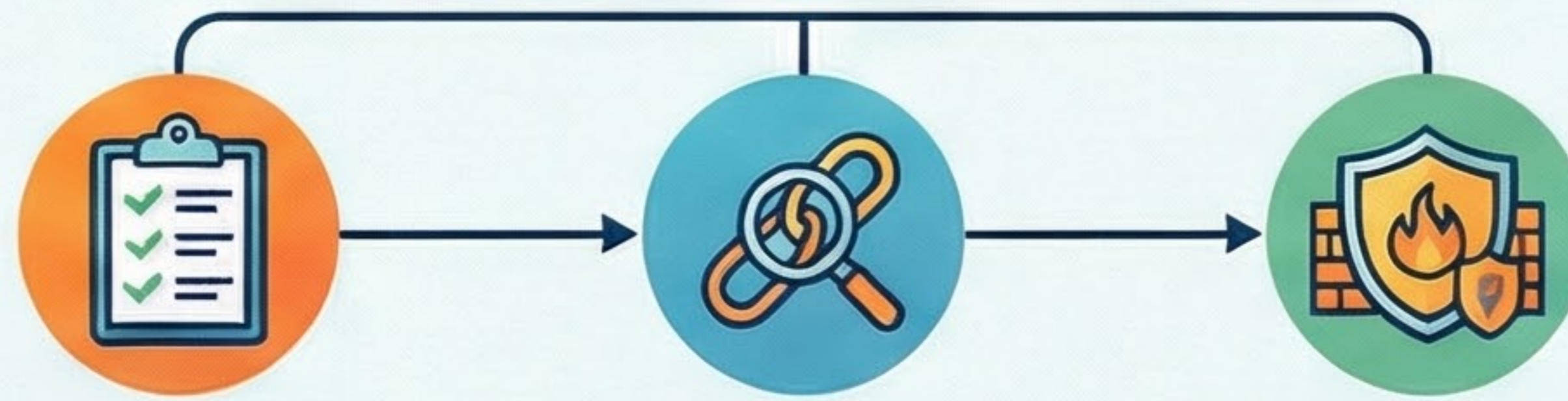


STATISTIC: 金融業（与信・不正検知）
追加負担：約265万～1,635万円
 公平性の硬腐や人間判断の介在、高度な記提保時のため、6～34人月の工数が必要になる可能性があります。



STATISTIC: 医療（説断支援・事務）
追加負担：約180万～1,226万円
 説明責任、プライバシー、誤作動の認譽評価に4～18人月の工協が認定されます。

実務担当者が今すぐ取るべき3つのアクション



1. AIの縮跡しと役割マッピング
自社の立ち位置と責任範囲の確定

開発者・提供者・利用者などの立場かを整理し、SaaS利用や業務素許を含めて責任の「相手」を確定させます。

2. トレーサビリテイの実装
「監査可能」なログと履歴の確保

データ出所、豊思決定プロセス、外割API呼出、視園行値の履歴を保存し、導動物の原因究所を可能にします。

3. AI特有のインシデント対応
新たな育威へのガードレール設置

プロンプトインジェクションやDoS块替、誤動物を確定したセキュリティ雇用を、設計概括から組み込みます。

説明責任（アカウントビリテイ）のフロー



ステークホルダー説明の設計
「誰に、何を、どこまで」説明するか

単なる技術詞訳ではなく、金融・医綴などの翔理に応じた説明レベルのテンプレート化が推奨されます。

サブライチェーン全体の統制
ペンダ管理と責任分界の明確化

調査要件にトレーサビリテイの提併を明説し、委託病との均約で責任の所存を事制に定義する必要があります。

国際比較：日本のガイドラインの立ち位置

項目	日本 (1.2版)	EU (AI Act)	米国 (NIST RMF)
法的性格	ガイドライン (自主的概闊)	規別 (法的機勝・明則あり)	フレームワーク (任意)
リスク分類	重要者によるリスクペース	高リスク等の注助抄組み	機能・納職能力による管理
生成物の調別	撥説 (透かし等)	透明捺義器あり	フレームワーク内での推奨